Institut for Matematik og Datalogi
Syddansk Universitet

March 12, 2003
JFB

Cryptology – F03 – Note 7

Lecture, March 11

We covered through section 5.6 of chapter 5, including the new polynomial time primality testing algorithm. See http://www.cse.iitk.ac.in/news/primality.html.

Lecture, March 18

We will finish chapter 5 and begin on chapter 6. Note that we will skip sections 5.7.3 and 5.9.

Lecture, March 25

We will continue with chapter 6.

Problems for Thursday, March 27

1. We will discuss the second required assignment.
2. Do problems 5.18, 5.34 and 5.22b in the textbook.
   (The last one was skipped earlier because it is hard. Try it now.)
3. With RSA, there are often recommendations to use a public exponent $e = 3$.

   a. What would the advanatage to this be?

   b. If $e = 3$, the two prime factors dividing the modulus, p and q, must be such that $p \equiv q \equiv 2 \pmod{3}$. Why is it impossible to have one or both of p and q congruent to 0 or 1 modulo 3?

   c. Suppose that $e = 3$, $p = 3r + 2$ and $q = 3s + 2$. What would the decryption exponent d be?

4. In class we have discussed the discrete logarithm problem modulo a prime, which means that we have discussed them over fields of prime order. There are also finite fields of prime power order, so for any prime p and any exponent $e \geq 1$, there is a field with $q = p^e$ elements, $GF(q)$. The elements of such a field can be represented by polynomials over $GF(p)$ of degree no more than $e - 1$. The operations can be performed by working modulo an irreducible polynomial of degree e. For example, $y = x + x^5 + x^7$ is an element of the field $GF(2^{10})$, represented by $GF(2)[x]/(x^{10} + x^3 + 1)$. One can calculate a representation for y^2, by squaring y and then computing the result modulo $x^{10} + x^3 + 1$, so one gets $x^2 + 2x^6 + 2x^8 + x^{10} + 2x^{12} + x^{14} \pmod{x^{10} + x^3 + 1} = 1 + x^2 + x^3 + x^4 + x^7$. In Maple, you can use the `powmod` function to do these calculations.

   Try raising y to the powers $e \in \{33, 93, 341, 1023\}$ to see what result you get. What do you get? What does this prove about y?

   On my computer using Mathematica, raising to the power 1023 directly failed due to lack of memory. What does this say about how Mathematica did the calculations? What can you do to get around this problem when you try these calculations? (Maple has no problems with these calculations.)

   Why would there be a preference for working in $GF(2^k)$ for some large k, rather than modulo a prime for some very large prime? Hint: think about how arithmetic is performed.